MiniCPS - A Toolkit for Security Research on CPS Networks

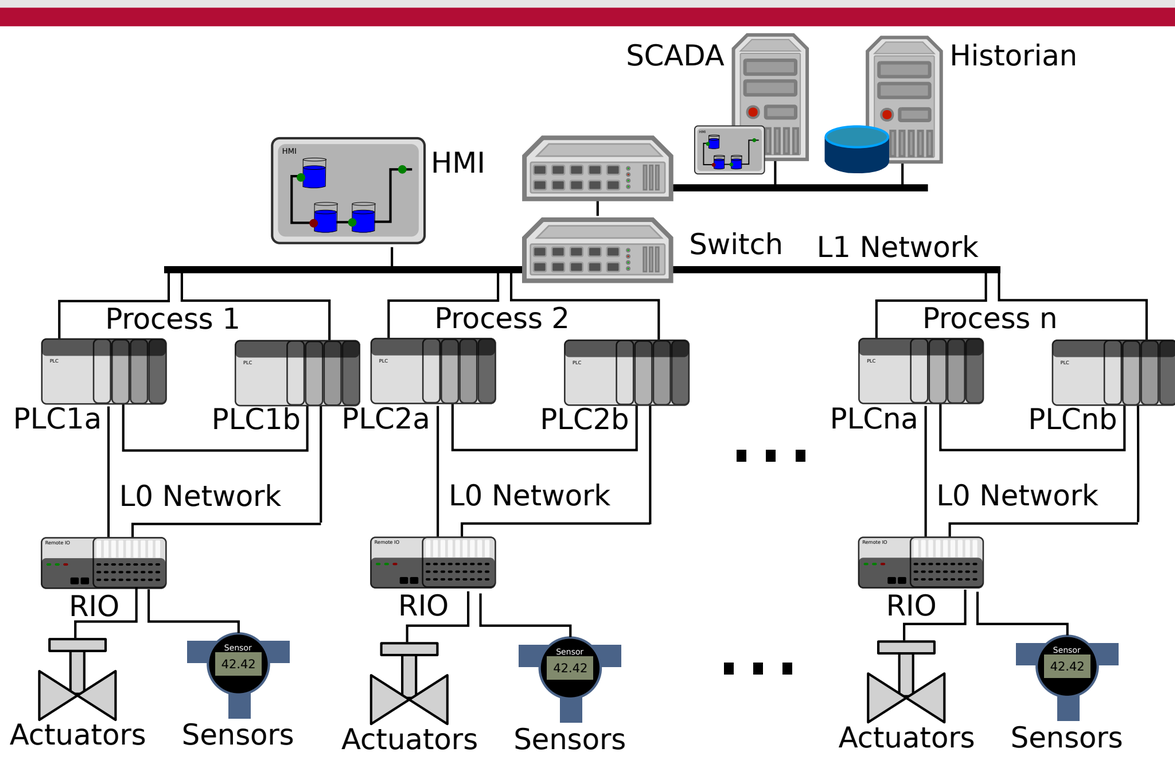
SINGAPORE UNIVERSITY OF TECHNOLOGY AND DESIGN
Established in collaboration with MIT

Daniele Antonioli and Nils Ole Tippenhauer

iTrust
Centre for Research in Cyber Security
CyPRO Protection of Cyber-Physical Systems

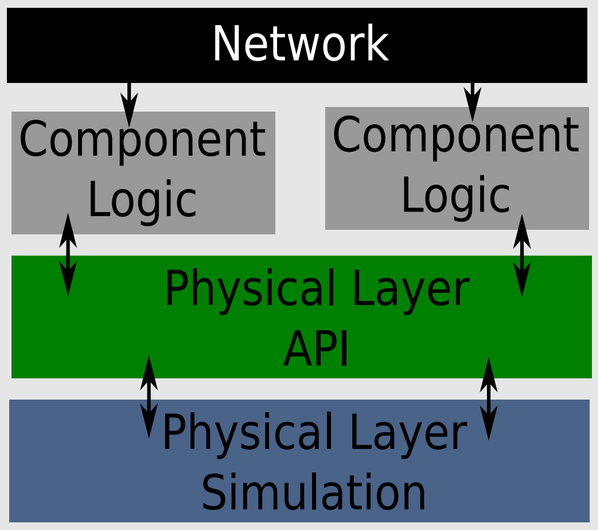
Problem Statement:

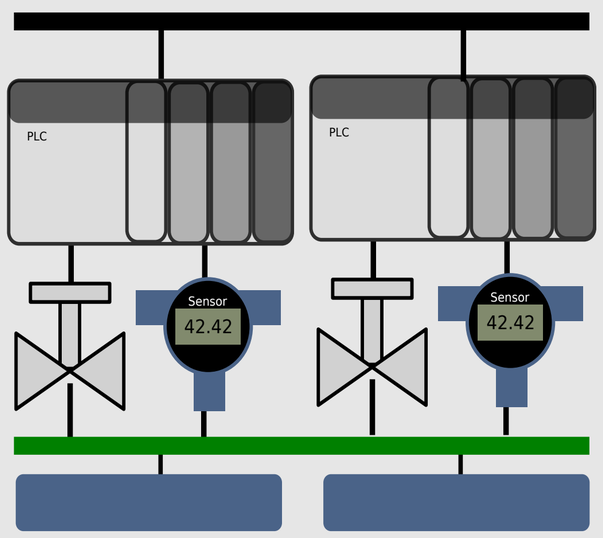
- Cyber-Physical Systems (CPS) Security is a major threat
- No simulation environment targeted to CPS research
- Physical Layer Interactions, Industrial Network Topologies
- Industrial Protocols: Ethernet/IP (CIP), Modbus/TCP.
- Simulation, emulation and co-simulation
- MiniCPS: Extensible, Reproducible CPS Research platform



MiniCPS:

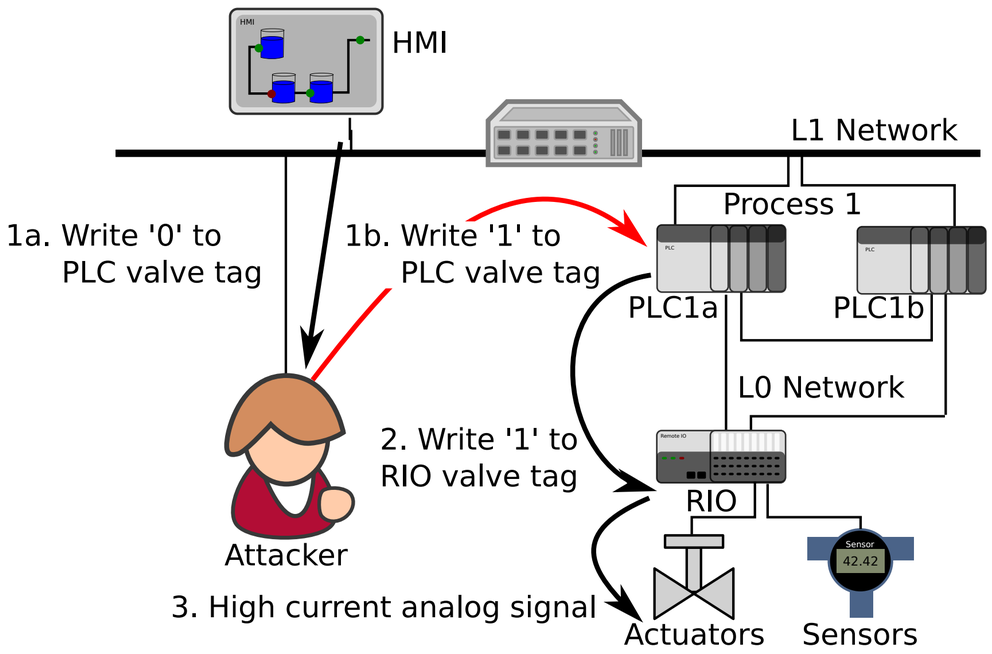
- Exchange Network Topologies and Configuration settings
- Test exploits and countermeasures in a safe but realistic manner
- Mininet emulator: lightweight, real traffic and SDN friendly (OpenFlow)
- Physical Process simulation scripts, e.g. MATLAB
- Component Logic simulation scripts, e.g Python





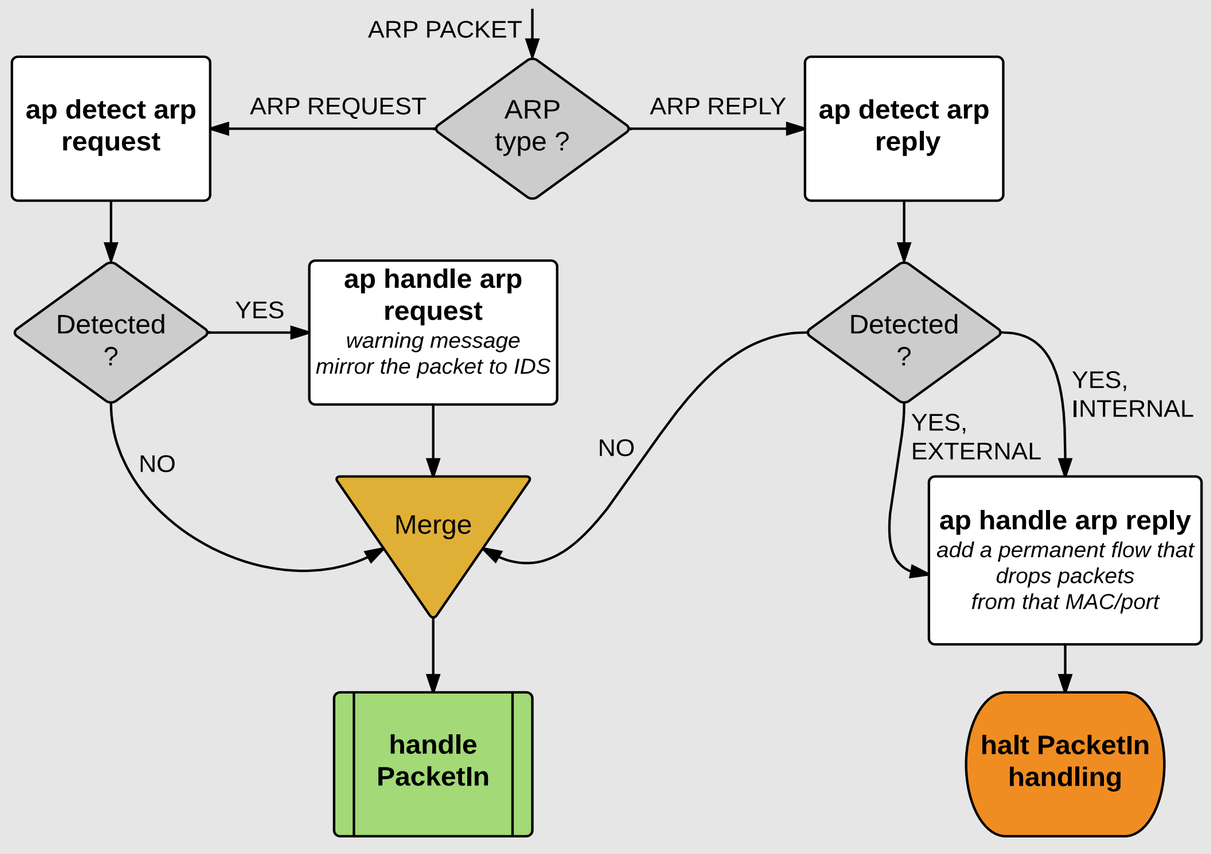
Man-in-the-Middle ARP spoofing Attacks:

- Designed and tested using MiniCPS. Validation on SUTD's Secure Water Treatment (SWaT) test bed
- Attacker between HMI and PLC1: custom ARP response packets to maintain the link
- Valve command is flipped Eg: HMI sends "open it" but PLC1 receives "close it"
- Water level is tampered Eg: PLC1 sends "overflow" but HMI receives "normal value"
- Simple, effective and stealthy using ettercap



Attack prevention using SDN:

- POX: event-driven, priority-based SDN framework.
- Attacker can both impersonate a new device or use an existing one (internal vs external)
- Attacker can both sniff the traffic and modify it on the fly (passive vs active)
- Controller pre-maps network addresses to set a known network state (proactive)
- Controller checks ARP suspicious packets and update the network state accordingly (reactive)
- Controller implements dedicated policy to mitigate the attack Eg: isolate the attacker



References:

"*MiniCPS: A Toolkit for Security Research on CPS Networks*" @ CPS-SPC '15: Proceedings of the First ACM Workshop on CPS Security and/or PrivaCy